UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	NO. 1:08CR239 (GBL)
	)	
ELAINE ROBERTSON CIONI	)	

MEMORANDUM IN SUPPORT OF MOTION TO DISMISS
COUNTS 1-4 OF THE INDICTMENT

Elaine Robertson Cioni, by counsel, submits the following Memorandum in support of her Motion to Dismiss Counts 1-4 of the Indictment.

On September 11, 2008, the government returned a superseding indictment charging the accused in multiple counts with accessing and attempting to access electronic mail accounts stored on protected computers in furtherance of gaining access to electronic mail stored on those computers in violation of Title 18 U.S.C. Sections 1030(a)(2)(C)and 2701, and conspiracy to do the same.

In particular, Count 1 of the Indictment charges, in pertinent part, that the accused conspired to violate the federal computer intrusion statutes. The conspiracy with which the accused is charged had as its purpose:

> "intentionally accessing protected computers without authorization (and exceeding authorized access to protected computers) in furtherance of intentionally gaining access without authorization (and exceeding authorized access to) to a facility through which an electronic communication service is provided and thereby obtaining electronic communications in electronic storage in violation of Title 18 United States Code, Sections 1030(a)(2)(C) and 2701." (emphasis added).[1]

[1] The protected computers referred to in Count 1 of the Indictment are computers that store electronic communications that are operated by AOL, Yahoo, Gmail and Hotmail.

Count 2 of the Superseding Indictment charges, in pertinent part, that beginning on or about November 20, 2006 and continuing until at least on or about March 10, 2008, the accused:

> "accessed and attempted to access, without authorization, a protected computer operated by AOL and obtained and attempted to obtain . . . ME's unopened electronic communications . . . in furtherance of a violation of Title 18, United States Code, Section 2701 [i.e., accessing a computer operated by AOL with out authorization and obtaining ME's unopened emails]." (emphasis added).

Count 3 of the Superseding Indictment charges in pertinent part that on various dates beginning on or around November 12, 2007 and continuing until at least on or around March 10, 2008, the accused:

> "gained and attempted to gain unauthorized access to the AOL account of PF . . . and attempted to obtain unopened electronic messages in PF's account . . . in furtherance of a violation of Title 18 United States Code, Section 371 [i.e., conspiracy to access protected computers containing email accounts in furtherance of intentionally gaining access to a facility through which email service is provided and thereby obtaining unopened emails]." (emphasis added).

Count 4 of the Superseding Indictment charges, in pertinent part, that on or about March 10, 2008, the accused:

> "intentionally attempted to access, without authorization, a protected computer operated by AOL. . . and obtain information contained in PF's electronic mail account . . . in furtherance of violations of Title 18, United States Code, Section 2701 [i.e., accessing a computer operated by AOL with out authorization and obtaining PF's unopened emails]." (emphasis added).

Ms. Cioni contends that Counts 1-4 fail to allege an offense and are multiplicitous in that each count charges her twice with a single offense.

Argument:

The constitutional guaranty established by the Double Jeopardy Clause protects against multiple punishments for the same offense. *United States v. Halper*, 490 U.S. 435, 440 (1989). In the multiple punishment context, the interest protected by the Double Jeopardy Clause "is

limited to ensuring that the total punishment did not exceed that authorized by the legislature." *United States v. Martin*, 523 F.3d 281, 290 (4th Cir. 2008), quoting *Jones v. Thomas*, 491 U.S. 376, 381 (1989). The protection services principally as a restraint on courts and prosecutors. See *United States v. Martin*, 523 F.3d at 290 (noting that "the root of the impact of the Double Jeopardy Clause on the legislature is the principle that the power to define criminal offenses and prescribe punishments upon those found guilty of them belongs solely to the legislature").

The longstanding test for multiplicity of charges was set down in *Blockburger v. United States*, 284 U.S. 299 (1932): "the applicable rule is that where the same act or transaction constitutes a violation of two distinct statutory provisions, the test to be applied to determine whether there are two offenses or only one, is that each provision requires proof of an additional fact which the other does not." *Id*. at 304. However, the Supreme Court made the point that the *Blockburger* rule is often easier to state than to apply when a splintered majority of the Supreme Court could not agree on how the test should be effectuated. See *United States v. Dixon*, 509 U.S. 688 (1993). While the *Blockburger* test focuses on the elements required to be proven under the applicable statutes, and not on the actual allegations in the indictment, see *United States v. Terry*, 86 F.3d 353, 356 (4th Cir. 1997), it is primarily a rule of statutory construction, and does not govern if the analysis is overcome by a clear indication of contrary legislative intent. *Abernaz v. United States*, 450 U.S. 333, 340 (1981).

In a case interpreting congressional intent in the context of a *Blockburger* analysis, the Fourth Circuit recently instructed that:

> Congress ordinarily does not intend to punish the same offense under two different statutes. Accordingly, where two statutory provisions proscribe the 'same offense.' they are construed not to authorize cumulative punishments in the absence of a clear indication of contrary legislative intent." (citation omitted).

United States v. Martin, 523 F.3d at 290. Only if the statute provides no definitive indication of congressional intent do courts apply the rule of statutory construction prescribed by the Supreme Count in *Blockburger*. *Id*.

Given this framework, this Court is required to examine the two provisions the accused is alleged to have been violated. Title 18 U.S.C. § 1030(a)(2)(C) proscribes intentionally accessing (or attempting to access) a protected computer, without authorization, and thereby obtaining information from a protected computer, if the conduct involves an interstate or foreign communication. The term "protected computer" includes a computer which is used in interstate or foreign commerce or communication. 18 U.S.C. §1030(e)(2)(B). The punishment for an offense under subsection (a)(2) is a fine, or imprisonment for not more than one year, or both. §1030 (c)(2)(A). However, the punishment for an offense under subsection (a)(2) is a fine or imprisonment for not more than five years, or both, if the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any state. §1030 (c)(2)(B) (ii).[2]

Title 18 U.S.C. §2701(a) proscribes intentionally accessing, without authorization, a facility through which an electronic communication service is provided and thereby obtaining access to electronic communications while it is in electronic storage (unopened). A provider of email accounts over the Internet is a provider of electronic communication service. See 18 U.S.C. § 2510(15); see also *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 560

[2] §1030 (c)(2)(B) also makes the punishment of an offense under subsection (a)(2) punishable by as a for not more than five years is the offense was committed for the purposes of commercial advantage or private financial gain, see §1030 (c)(2)(B)(I) or, the value of the information obtained exceeds $5000, see §1030 (c)(2)(B)(iii).

(N.D.Cal.2000). If the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State, the punishment for an offense under subsection (a)(2) is a fine or imprisonment for not more than five years, or both. § 2701(b)(1)(A). In any other case, the punishment for an offense under subsection (a)(2) is a fine or imprisonment for not more than one year, or both. § 2701(b)(2)(A).

Thus, in the case of both statutes, felony charges require proof of an additional element: that the accused acted "for commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act." This element was added to Section 2701 by the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002). Originally, Section 1030(a)(2) protected individual privacy by criminalizing unauthorized access to computerized information and credit records relating to customers' relationships with financial institutions. See S. Rep. No. 99-432 at 6 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2483; see also S. Rep. 104-357, at 7; *America Online, Inc. v. National Health Care Discount, Inc*. 1221 F. Supp. 2d 1255, 1275 (N.D. Iowa 2000). In 1996, Congress expanded the scope of the section by adding two subsections that also protected information on government computers (§ 1030(a)(2)(B)) and computers used in interstate or foreign communication (§ 1030(a)(2)(C)), the offense with which the accused is charged. Clearly, to increase the punishment from one to five years, the prohibited purpose must be the accused's primary motivation or at least a determinative factor in the accused's motivation. See *United States v. Cassiere*, 4 F.3d 1006, 1021 (1st Cir.1993).

It should be obvious beyond peradventure that the prohibited purpose harbored by the

accused must be a purpose other than the accessing of unlawfully accessing stored electronic communications. The Department of Justice Computer Crime & Intellectual Property Section Manual recognized this precept stating that:

> "Naturally, the 'in furtherance of any criminal or tortious act' language means an act other than the unlawful access to stored communications itself. See *Boddie v. American Broadcasting Co.*,731 F.2d 333, 339 (6th Cir. 1984)." (emphasis added).[3]

It is precisely that that the Superseding Indictment purports to do.

It should be equally clear that *Blockburger* cannot be satisfied simply by the use of different, although technically indistinguishable statutory terms which the Superseding Indictment also seeks to do. For example, Count 2 of the Superseding Indictment charges the accused with intentionally accessing, without authorization, a protected computer operated by AOL. . . and obtaining information contained in an electronic mail account . . . in furtherance of violations of Title 18, United States Code, Section 2701, i.e., accessing a computer operated by AOL with out authorization and obtaining unopened emails. It is clear that in the circumstances of this case, the parallel elements of § 1030 and § 2701 are indistinguishable for the purposes of *Blockburger*. Consequently, the Court is required to conclude that, as alleged in the Superseding Indictment, § 1030 does not require proof of a fact distinct from § 2701 and cannot serve as the separate and distinct prohibited purpose and vice versa.

Moreover, even if the accused were to concede a hypothetical difference in the elements of the two crimes, "the [Blockburger] rule should not be controlling where, for example, there is a clear indication of contrary legislative intent." *Missouri v. Hunter*, 459 U.S. 359, 367 (1983). Requiring proof in both statutes of an additional element in order to elevate a misdemeanor

---

[3] The CCIPS Manual can be accessed at http://www/cybercrim.gov/ccmanual/01ccma.html.

offense to a felony is a clear indication of contrary legislative intent.

WHEREFORE, for the foregoing reasons and such additional reasons as may be argued at a hearing on this motion, the accused requests this Court dismiss Counts 1-4 of the Superseding Indictment.

Respectfully submitted,

ELAINE ROBERTSON CIONI
By Counsel

/s/

Nina J. Ginsberg, Esquire
VSB # 19472
Counsel for Elaine Robertson Cioni
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: 703-684-4333
Fax: 703-548-3181
nginsberg@dimuro.com

CERTIFICATE OF SERVICE

I hereby certify that on October 3, 2008, I will electronically file the foregoing pleading with the Clerk of Court using the CM/ECF system, which will then send a notification of such

filing (NEF) to:

Jay Prabhu, Esquire
Assistant U.S. Attorney
2100 Jamieson Avenue
Alexandria, VA 22314
703-299-3700
jay.prabhu@usdoj.gov

/s/
Nina J. Ginsberg, Esquire
VSB # 19472
Counsel for Elaine Robertson Cioni
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: 703-684-4333
Fax: 703-548-3181
nginsberg@dimuro.com